IN THE SPECIFICATION:

The specification as amended below with replacement paragraphs shows added text with underlining and deleted text with ~~strikethrough~~.

Please REPLACE the paragraph at page 38, lines 1-5, with the following paragraph:

TABLE 2. Relation between Mask Value and Amount of Computation Required for Determining 128-bit Secret Key by DPA of Loading Sbox ~~Output~~ Input Values, for One Common Sbox Set for Subbytes, in Fixed Mask Value Method.

Please REPLACE the paragraph at page 41, lines 1-15, with the following paragraph:

The F function of FIGURE 33B includes a selector 759 for providing a fixed mask value $FM_{i,h}$ selected in response to the random number h, an XOR 762 for XORing the sub-key K_i with the fixed mask value $FM_{i,h}$ to provide an output, an XOR 763 for XORing the output value with an input Xi' linearly transformed by a linear transform E, selectors 752 to 756 for selecting one of Subbytes [[$S_{i,h}$]] $S_{j,h}$ in response to the random number h to provide the output from the XOR 763, Subbytes [[$S_{i,h}$]] $S_{j,h}$ for performing the Subbyte in accordance with the respective nonlinear table Sboxes [[$S_{i,h}$]] $S_{j,h}$, selectors 754 to 757 for selecting one of the Subbytes [[$S_{i,h}$]] $S_{j,h}$ in response to the random number h to provide an output, and a linear transform P for linearly transforming the output from the selectors 754 to 757 to provide an output Zi'.

Please REPLACE the paragraph at page 42, lines 24-30, with the following paragraph:

The F function of FIGURE 34B includes an XOR 862 for XORing the input Xi' linearly transformed by a linear transform E with the XOR value of the sub-key K_i with the fixed mask value $FM_{i,h}$, Subbytes [[$S_{i,h}$]] $S_{j,h}$ (i = 1, 2, ... 8) in accordance with the nonlinear table SBoxes $S_{i,h}$, and a linear transform P for linearly transforming the output from the Subbyte [[$S_{i,h}$]] $S_{j,h}$ to provide an output Zi'.